Express Mail Label No. Dated: _____

Docket No.: 20046/0200957-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Jean-Pierre Seifert et al.

Application No.: 10/789,373 Confirmation No.:

Filed: February 27, 2004 Art Unit: N/A

For: DEVICE AND METHOD FOR CALCULATING A RESULT OF MODULAR EXPONENTIATION Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Germany	101 43 728.5	September 6, 2001

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 25, 2004

Respectfully submitted,

By Pl-Rec Basses (53,970)
Laura C. Brutman
Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 753-6237 (Fax)
Attorneys/Agents For Applicant

03-26-04

Application No. (if known): 10/789,373 Attorney Docket No.: 20046/0200957-US0

Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV983947001-US in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on March 25, 2004
Date

Signature

D B Peck

Typed or printed name of person signing Certificate

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

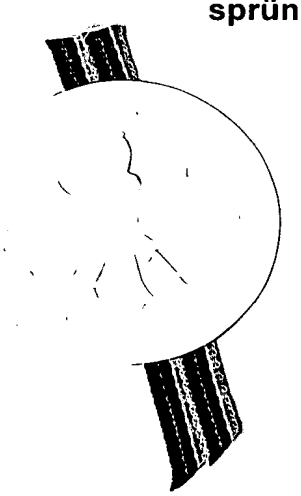
Claim for Priority & Submission of Documents
DE 101 43 728.5
Return Receipt Postcard

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	101 43 728.5
Anmeldetag:	06. September 2001
Anmelder/Inhaber:	Infineon Technologies AG, 81669 München/DE
Bezeichnung:	Vorrichtung und Verfahren zum Berechnen eines Ergebnisses einer modularen Exponentiation
IPC:	H 04 L 9/30

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.



München, den 4. März 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Wallner

A 9161
06/00
EDV-L

SCHOPPE, ZIMMERMANN, STÖCKELER & ZINKLER

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Patentanwälte · Postfach 710867 · 81458 München

Infineon Technologies AG
St.-Martin-Str. 53

81669 München

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.
Franz Zinkler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977
e-mail: szsz_iplaw@t-online.de

Vorrichtung und Verfahren zum Berechnen eines Ergebnisses einer modularen Exponentiation

Beschreibung

Vorrichtung und Verfahren zum Berechnen eines Ergebnisses einer modularen Exponentiation

Die vorliegende Erfindung bezieht sich auf die modulare Exponentiation und insbesondere auf die modulare Exponentiation unter Verwendung des chinesischen Restsatzes (CRT; CRT = Chinese Residue Theorem).

Bevor näher auf das RSA-Kryptosystem eingegangen wird, seien zunächst einige Grundbegriffe der Kryptographie zusammengefaßt. Allgemein unterscheidet man zwischen symmetrischen Verschlüsselungsverfahren, die auch als Secret-Key-Verschlüsselungsverfahren bezeichnet werden, und Public-Key-Verschlüsselungsverfahren, welche auch als Verschlüsselungsverfahren mit öffentlichem Schlüssel bezeichnet werden.

Ein Kommunikationssystem mit zwei Parteien, welche eine Verschlüsselung mit symmetrischem Schlüssel verwenden, kann folgendermaßen beschrieben werden. Die erste Partei teilt ihren Verschlüsselungsschlüssel über einen sicheren Kanal der zweiten Partei mit. Dann verschlüsselt die erste Partei die geheime Nachricht mittels des Schlüssels und überträgt die verschlüsselte Nachricht über einen öffentlichen oder nichtgesicherten Kanal zu der zweiten Partei. Die zweite Partei entschlüsselt dann die verschlüsselte Nachricht unter Verwendung des symmetrischen Schlüssels, der der zweiten Partei über den gesicherten Kanal mitgeteilt worden ist. Ein wesentliches Problem bei solchen Verschlüsselungssystemen besteht darin, ein effizientes Verfahren zum Austauschen der geheimen Schlüssel, d. h. zum Finden eines sicheren Kanals, zu schaffen.

Bei der asymmetrischen Verschlüsselung wird hingegen folgendermaßen vorgenommen. Eine Partei, die eine geheime Nachricht erhalten möchte, teilt ihren öffentlichen Schlüssel der ande-

ren Partei, d. h. der Partei, von der sie eine geheime Nachricht erhalten möchte, mit. Der öffentliche Schlüssel wird über einen nicht-gesicherten Kanal, also über einen „öffentlichen" Kanal mitgeteilt.

Die Partei, die eine geheime Nachricht abschicken möchte, empfängt den öffentlichen Schlüssel der anderen Partei, verschlüsselt die Nachricht unter Verwendung des öffentlichen Schlüssels und sendet die verschlüsselte Nachricht wieder über einen nicht-gesicherten Kanal, also über einen öffentlichen Kanal, zu der Partei, von der der öffentliche Schlüssel stammt. Lediglich die Partei, die den öffentlichen Schlüssel erzeugt hat, ist in der Lage, einen privaten Schlüssel bereitzustellen, um die verschlüsselte Nachricht zu entschlüsseln. Nicht einmal die Partei, die unter Verwendung des öffentlichen Schlüssels ihre Nachricht verschlüsselt hat, ist in der Lage, die Nachricht zu entschlüsseln. Ein Vorteil dieses Konzepts besteht darin, daß zwischen den beiden Parteien kein gesicherter Kanal, also kein geheimer Schlüsselaustausch erforderlich ist. Die Partei, die die Nachricht verschlüsselt hat, muß und darf den privaten Schlüssel des Nachrichtenempfängers nicht kennen.

Ein physikalisches Analogon zum asymmetrischen Verschlüsselungskonzept oder Public-Key-Verschlüsselungskonzept stellt sich folgendermaßen dar. Es sei eine Metallkiste betrachtet, deren Deckel durch ein Kombinationsschloß gesichert ist. Die Kombination kennt nur die Partei, die eine verschlüsselte Nachricht erhalten möchte. Wenn das Schloß offen gelassen wird und öffentlich verfügbar gemacht wird, dann kann jeder, der eine geheime Nachricht absetzen will, diese Nachricht in die Metallkiste hinein legen und den Deckel verschließen. Nur der, von dem die Kiste stammt, kennt jedoch die Kombination des Kombinationsschlosses. Nur er ist in der Lage, die Nachricht zu entschlüsseln, d. h. die Metallkiste wieder zu öffnen. Selbst der, der die Nachricht in die Kiste hineingelegt

hatte, ist nicht mehr in der Lage, dieselbe wieder herauszuholen.

Wesentlich für asymmetrische oder Public-Key-Verschlüsselungskonzepte ist das zugrunde liegende mathematische Problem, dessen Lösung unter Verwendung des öffentlichen Schlüssels zur Entschlüsselung nahezu unmöglich ist, dessen Lösung jedoch unter Kenntnis des privaten Schlüssels leicht möglich ist. Eines der bekanntesten Public-Key-Kryptosysteme ist das RSA-Kryptosystem. Das RSA-Kryptosystem ist im „Handbook of Applied Cryptography", Menezes, van Oorschot, Vanstone, CRC Press 1997, Seiten 285-291 beschrieben.

Anschließend wird auf Fig. 3 Bezug genommen, um den RSA-Algorithmus darzustellen. Ausgangslage ist, daß ein Kommunikationspartner eine Nachricht m verschlüsselt, die der andere Kommunikationspartner wieder entschlüsseln muß. Die verschlüsselnde Entität muß zunächst in einem Schritt 200 den öffentlichen Schlüssel (n, e) erhalten, um der anderen Partei überhaupt eine verschlüsselte Nachricht schicken zu können. Daran anschließend muß die verschlüsselnde Entität in einem Schritt 210 die zu verschlüsselnde Nachricht als Ganzzahl m darstellen, wobei m in dem Intervall von 0 bis n-1 liegen muß. In einem Schritt 220, welcher der eigentliche Verschlüsselungsschritt ist, muß die verschlüsselnde Entität folgende Gleichung berechnen:

$$c = m^e \bmod n.$$

c ist die verschlüsselte Nachricht. Diese wird dann in einem Schritt 230 ausgegeben und über einen öffentlichen Kanal, der in Fig. 2 mit 240 bezeichnet ist, zu dem Empfänger der verschlüsselten Nachricht übertragen. Dieser empfängt in einem Schritt 250 die verschlüsselte Nachricht c und führt in einem Schritt 260, welcher der eigentliche Entschlüsselungsschritt ist, folgende Berechnung durch:

$m = c^d \bmod n.$

Aus Fig. 3 ist zu sehen, daß zum Verschlüsseln lediglich der öffentliche Schlüssel (n, e) benötigt wird, jedoch nicht der private Schlüssel d, während beim Entschlüsseln der private Schlüssel d benötigt wird.

Fraglich ist nun, wie ein Angreifer ein RSA-Kryptosystem brechen kann. Ihm ist der öffentliche Schlüssel, also n und e bekannt. Er könnte nunmehr den Modul n in ein Produkt von zwei Primzahlen faktorisieren und dann den geheimen Schlüssel d genauso berechnen, wie es die Schlüssel-erzeugende authentische Partei gemacht hat. Der Angreifer müßte hierzu sämtliche mögliche Primzahlenpaare p´, q´ durchprobieren, um dann irgendwann unter Berücksichtigung von e auf den privaten Schlüssel d zu stoßen. Bei kleinen Primzahlen p und q ist dieses Problem relativ leicht einfach durch Durchprobieren zu lösen. Werden jedoch p und q, also der Modul n, der ja gleich der Produkt aus p und q ist, immer größer, so steigen die verschiedenen Möglichkeiten für die Faktorisierung des Moduls n in astronomische Höhen. Hierauf basiert die Sicherheit des RSA-System. Daraus ist zu sehen, daß ein sicheres RSA-Kryptosystem sehr lange Zahlen verwenden muß, welche beispielsweise 512, 1024 oder aber bis zu 2048 Bit lang sein können.

Aus Fig. 3 ist zu sehen, daß sowohl für eine RSA-Verschlüsselung, um aus einer nicht-verschlüsselten Nachricht m eine verschlüsselte Nachricht c zu erzeugen, als auch zum Entschlüsseln, also um aus einer verschlüsselten Nachricht c eine entschlüsselte Nachricht m zu erzeugen, eine modulare Exponentiation berechnet werden muß. Dies wird in Fig. 3 durch die Schritte 220 und 260 deutlich. Bei der Berechnung der modularen Exponentiation ist insbesondere dann der chinesische Restsatz (CRT) günstig, wenn die verwendeten Ganzzahlen, und insbesondere der Modul n lange Zahlen sind. Wie es

ausgeführt worden ist, basiert jedoch die Sicherheit des RSA-Algorithmus darauf, daß die Ganzzahlen lang sind.

Der chinesische Restsatz ist in dem „Handbook of Applied Cryptography, das vorher erwähnt wurde, auf Seite 610 ff beschrieben. Der chinesische Restsatz und insbesondere in seiner Ausprägung, die als Garner´s Algorithmus bekannt ist, basiert darauf, die modulare Exponentiation mit dem Modul n auf zwei modulare Exponentiationen zweiter Untermodule p, q aufzuspalten, wobei die Untermodule p, q Primzahlen sind und wobei das Produkt derselben den Modul n ergibt. Eine modulare Exponentiation mit einem langen Modul wird somit auf zwei modulare Exponentiationen mit kürzeren (typischerweise halb so langen) Untermodulen zerlegt. Dieses Verfahren ist darin vorteilhaft, daß lediglich halb so lange Rechenwerke benötigt werden bzw. daß, bei gleichbleibender Länge eines Rechenwerks doppelt so lange Zahlen verwendet werden können, was in einem günstigeren Verhältnis von Sicherheit zu Chipfläche, also allgemein in einem besseren Verhältnis von Leistung zu Preis resultiert.

Der chinesische Restsatz angewendet auf die beschriebene modulare Exponentiation stellt sich folgendermaßen dar. Zunächst werden zwei Primzahlen pq ermittelt, die möglichst nahezu gleich lang sein sollten, und deren Produkt p x q den Modul n ergibt. Anschließend wird eine erste Hilfsgröße dp folgendermaßen berechnet:

$$dp = d \bmod (p - 1).$$

Hierauf wird eine zweite Hilfsgröße dq berechnet:

$$dq = d \bmod (q - 1).$$

Daran anschließend wird eine dritte Hilfsgröße Mp berechnet:

$$Mp = c^{dp} \bmod p.$$

Eine weitere Hilfsgröße Mq wird folgendermaßen berechnet:

$$Mq = c^{dq} \bmod q.$$

In einem abschließenden Zusammenfassungsschritt wird schließlich das Ergebnis der modularen Exponentiation, d. h. im vorliegenden Beispiel die Klartext-Nachricht m folgendermaßen berechnet, wenn c die verschlüsselte Nachricht ist:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q$$

Aus der vorangehenden Darstellung des chinesischen Restsatzes ist zu sehen, daß eine modulare Exponentiation mit einem langen Modul n in zwei modulare Exponentiationen mit halb so langen Untermodulen p, q zerlegt worden ist, und daß dann, im letzten Schritt, um die Klartextnachricht m zu berechnen, eine Zusammenfassungsoperation ausgeführt wird, in der die multiplikative Inverse q^{-1} bezüglich eines Untermoduls p benötigt wird. Nachdem der Untermodul p kürzer als der ursprüngliche Modul n ist, ist auch die Berechnung der multiplikativen Inversen q^{-1} z. B. unter Verwendung des erweiterten Euklidschen Algorithmus, mit vertretbarem Rechenaufwand möglich.

Obgleich die Verwendung des chinesischen Restsatzes die Rechenzeiteffizienz bzw. den Chipflächenverbrauch eines Sicherheits-IC reduziert, birgt der chinesische Restsatz Probleme durch Angriffe auf das Kryptographiesystem, wie z. B. sogenannten Side-Channel-Attacken, Leistungsanalysen oder Fehlerattacken. Ein Angreifer könnte solche Attacken auf den Algorithmus ausführen, um den privaten Schlüssel d zu „knacken".

Im Falle der RSA-Verschlüsselung, also wenn aus der Klartextnachricht m eine verschlüsselte Nachricht c berechnet werden soll, ist das Sicherheitsproblem nicht derart evident, da zur

Verschlüsselung einer Nachricht ohnehin nur der öffentliche Schlüssel e verwendet wird. Jedoch tritt das Problem bei der Verwendung von RSA als Signaturalgorithmus auf.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein sicheres und effizientes Konzept zur Berechnung der modularen Exponentiation zu schaffen, das die RSA-Signatur mittels CRT gegen Fehlerattacken schützt.

Diese Aufgabe wird durch eine Vorrichtung zum Berechnen eines Ergebnisses einer modularen Exponentiation gemäß Patentanspruch 1 oder 6 oder durch eine Vorrichtung zum Berechnen eines Ergebnisses einer modularen Exponentiation gemäß Patentanspruch 9 oder 10 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß die Sicherheit der modularen Exponentiation, die die Basisoperation für RSA-Verschlüsselungen ist, auch dann erhöht werden kann, wenn der chinesische Restsatz eingesetzt wird, um die RSA-Exponentiation effizienter berechnen zu können. Dies wird dadurch erreicht, daß benötigte Hilfsgrößen für den chinesischen Restsatz randomisiert werden bzw. daß ein Sicherheitsparameter bei den modularen Exponentiationen für die Untermodule eingeführt wird. Die Randomisierung der Exponenten und/oder die durch den Sicherheitsparameter bewirkte Veränderung des Moduls der beiden „Hilfs-Exponentiationen" des chinesischen Restsatzes liefern eine erhöhte Sicherheit gegen Side-Channel-Attacken oder Fehlerattacken.

Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, daß bestehende Kryptoprozessoren, mit denen unter Verwendung des CRT die RSA-Exponentiation berechnet werden kann, nicht modifiziert werden müssen, sondern daß lediglich die CRT-Standardparameter modifiziert werden müssen, jedoch nicht die zentralen Rechenschritte zur Berechnung der beiden modularen Exponentiationen unter Verwendung der Untermodule.

Dies bedeutet, daß sämtliche vorhandenen Strukturen für die Schlüsselverwaltung der RSA-Schlüssel weiter benutzt werden können.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

Fig. 1 eine Vorrichtung zum Berechnen der modularen Exponentiation gemäß einem ersten Ausführungsbeispiel der vorliegenden Erfindung, bei dem die Exponenten der Hilfs-Exponentiationen randomisiert sind;

Fig. 2a einen Ausschnitt einer Vorrichtung zum Berechnen der modularen Exponentiation gemäß einem zweiten Ausführungsbeispiel der vorliegenden Erfindung, das entweder allein oder zusammen mit dem ersten Ausführungsbeispiel der vorliegenden Erfindung verwendet werden kann, wobei die Untermodule randomisiert sind;

Fig. 2b eine Fehlerüberprüfungstechnik zum Überprüfen der Ergebnisse der Hilfs-Exponentiationen vor der Zusammenfassung der Ergebnisse; und

Fig. 3 ein schematisches Flußdiagramm des RSA-Algorithmus zur Verschlüsselung und zur Entschlüsselung.

Fig. 1 zeigt eine erfindungsgemäße Vorrichtung zum sicheren Berechnen des Ergebnisses einer modularen Exponentiation unter Verwendung des chinesischen Restsatzes. Eingangsparameter sind zwei Primzahlen p, q, deren Produkt den Modul n der modularen Exponentiation ergeben. Ein weiterer Eingabeparameter ist der Schlüssel d. Im nachfolgenden wird das erste Ausführungsbeispiel der vorliegenden Erfindung anhand der Entschlüsselung beim RSA-Algorithmus dargestellt. Aus einer verschlüsselten Nachricht c wird unter Verwendung des privaten

Schlüssels d die entschlüsselte Nachricht m gemäß folgender Gleichung berechnet:

$$m = c^d \bmod n.$$

Die erfindungsgemäße Vorrichtung umfaßt eine Einrichtung 100 zum Berechnen der ersten Hilfsgröße dp gemäß folgender Gleichung:

$$dp = d \bmod (p - 1).$$

Eine weitere Einrichtung 102 zum Berechnen einer zweiten Hilfsgröße dq führt folgende Gleichung aus:

$$dq = d \bmod (q - 1).$$

Die erfindungsgemäße Vorrichtung zum Berechnen eines Ergebnisses einer modularen Exponentiation umfaßt ferner eine Einrichtung 104 zum Erzeugen einer Zufallszahl IRND 104. Dieser Einrichtung ist wiederum eine Einrichtung 106 nachgeschaltet, um eine dritte Hilfsgröße dp´ gemäß folgender Gleichung zu berechnen:

$$dp' = IRND \times (p - 1) + dp.$$

Die dritte Hilfsgröße dp´ ist somit ein randomisierter Exponent der ersten Hilfs-Exponentiation, die mittels einer Einrichtung 110 zum Berechnen der fünften Hilfsgröße Mp berechnet wird, die ausgebildet ist, um folgende Gleichung auszuführen:

$$Mp = c^{dp'} \bmod p.$$

Analog hierzu ist eine Einrichtung 108 vorgesehen, um eine vierte Hilfsgröße dq´ gemäß folgender Gleichung zu berechnen:

$$dq' = IRND (q - 1) + dq.$$

Mittels der vierten Hilfsgröße, die den randomisierten Exponenten der zweiten Hilfs-Exponentiation darstellt, arbeitet eine Einrichtung 112 zum Berechnen der sechsten Hilfsgröße Mq:

$$Mq = c^{dq'} \bmod q.$$

Eine Einrichtung 114 berechnet schließlich das Ergebnis m, d. h. im vorliegenden Beispiel die entschlüsselte Nachricht, gemäß folgender Gleichung:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

Die für den RSA-Algorithmus benötigte modulare Exponentiation kann ferner sicherer gestaltet werden, wenn der Hilfsmodul d bzw. der Hilfsmodul q verändert werden. Dies ist in Fig. 2a dargestellt. Eine Vorrichtung gemäß einem zweiten Ausführungsbeispiel der vorliegenden Erfindung umfaßt eine Einrichtung 120 zum Erzeugen einer Primzahl T als Sicherheitsparameter, die vorzugsweise eine relativ kleine Primzahl ist, damit der Rechenzeitvorteil des chinesischen Restsatzes nicht zugunsten der Sicherheit zu stark „geopfert" wird. Das Ergebnis der ersten Hilfs-Exponentiation Mp wird dann genauso wie das Ergebnis der zweiten Hilfs-Exponentiation Mq nicht unter Verwendung der ursprünglichen Hilfs-Untermodule p, q, sondern unter Verwendung der mit dem Sicherheitsparameter beaufschlagten Hilfs-Untermodule p x T bzw. q x T durch die Einrichtungen 110´ bzw. 112´ berechnet. Bereits die Veränderung der Untermodule p, q alleine, also ohne Randomisierung der Hilfs-Exponenten dp´ bzw. dq´ liefert eine erhöhte Sicherheit gegenüber kryptographischen Attacken. Die sicherste Variante gemäß der vorliegenden Erfindung besteht jedoch darin, sowohl die Randomisierung der Hilfs-Exponenten, wie in Fig. 1 dargestellt, als auch die veränderten Hilfs-Module, wie es in Fig. 2a dargestellt ist, zu verwenden. In diesem Fall würde die Vorrichtung zum Berechnen eines Ergebnisses einer modularen

Exponentiation wie in Fig. 1 dargestellt ausgebildet sein, jedoch mit dem Unterschied, daß die Einrichtung 120 vorgesehen ist, und die Einrichtung 110 und 112 von Fig. 1 statt der Untermodule p, q die mit dem Sicherheitsparameter beaufschlagten Untermodule pT bzw. qT verwenden.

Die Verwendung der mit dem Sicherheitsparameter beaufschlagten Untermodule zusammen mit den randomisierten Exponenten ermöglicht es, wie es in Fig. 2b dargestellt ist, vor der Berechnung des Ergebnisses unter Verwendung der Einrichtung 114 von Fig. 1 eine Hilfs-Berechnung durchzuführen, wie sie im Block 140 von Fig. 2b dargestellt ist. Wenn diese Gleichung erfüllt ist, kann eine Ausgabe erfolgen, daß der chinesische Restsatz (CRT) korrekt ausgeführt ist (Block 142).

Ist die durch die Einrichtung 140 dargestellte Gleichheitsbedingung nicht erfüllt, kann eine Ausgabe 144 erfolgen. Tritt ein CRT-Fehler auf, so kann die Rechnung bereits hier vor der „Zusammenfassung" durch die Einrichtung 114 abgebrochen werden. Weiterhin ist ferner sichergestellt, daß die randomisierten Hilfsexponenten dp´ und dq´ auf die durch den Sicherheitsparameter veränderten Untermodule pT bzw. qT abgestimmt sind, wenn, wie es bevorzugt wird, sowohl die Hilfs-Exponenten randomisiert werden als auch die Untermodule verändert werden. Als Sicherheitsparameter T wird im Sinne eines Kompromisses zwischen CRT-Rechenersparnis und Sicherheit aufgrund der verlängerten Untermodule die relative kleine Primzahl 32771 bevorzugt.

Die Zwischenergebnisüberprüfung durch die Einrichtung 140 stellt sicher, dass bereits vor Ausgabe eines Ergebnisses der Algorithmus abgebrochen wird, wenn beispielsweise während der Berechnung von M_p und/oder M_q eine Fehlerattacke auf den Sicherheits-IC ausgeführt worden ist. Diese Attacke wird scheitern, da im Falle einer solchen Attacke „CRT-Fehler" durch die Einrichtung 140 erzeugt wird, so dass keine Ausgabe erfogen wird und die Fehlerattacke somit ins Leere geht. Des Wei-

teren sei darauf hingewiesen, dass dieser Schutz durch die Zwischenergebnisprüfung relativ wenig aufwendig ist, da der Parameter T vorzugsweise eine kleine Primzahl ist, so dass die Exponentiation im Block 140 von Fig. 2b einen im Vergleich zum Modul kleinen Exponenten hat.

Patentansprüche

1. Vorrichtung zum Berechnen eines Ergebnisses einer modularen Exponentiation, wobei n ein Modul ist, wobei d ein Exponent ist, und wobei c eine Größe ist, die der modularen Exponentiation zu unterziehen ist, mit folgenden Merkmalen:

einer Einrichtung (100) zum Berechnen einer ersten Hilfsgröße dp, wobei dp folgendermaßen definiert ist:

$$dp = d \bmod (p - 1),$$

wobei p eine erste Primzahl ist;

einer Einrichtung (102) zum Berechnen einer zweiten Hilfsgröße dq, wobei dq folgendermaßen definiert ist:

$$dq = d \bmod (q - 1),$$

wobei q eine zweite Primzahl ist,

wobei ein Produkt aus p und q gleich dem Modul n ist;

einer Einrichtung (104) zum Erzeugen einer Zufallszahl (IRND);

einer Einrichtung (106) zum Erzeugen einer dritten Hilfsgröße dp´, wobei dp´ folgendermaßen definiert ist:

$$dp' = IRND \times (p - 1) + dp;$$

einer Einrichtung (108) zum Erzeugen einer vierten Hilfsgröße dq´, wobei dq´ folgendermaßen definiert ist:

$$dq' = IRND \times (q - 1) + dq;$$

einer Einrichtung (110) zum Erzeugen einer fünften Hilfsgröße Mp, wobei die fünfte Hilfsgröße Mp folgendermaßen definiert ist:

$$Mp = c^{dp'} \bmod p;$$

einer Einrichtung (112) zum Erzeugen einer sechsten Hilfsgröße Mq, wobei die sechste Hilfsgröße Mq folgendermaßen definiert ist:

$$Mq = c^{dq'} \bmod q; \text{ und}$$

einer Einrichtung (114) zum Berechnen des Ergebnisses der modularen Exponentiation m, wobei m folgendermaßen definiert ist:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

2. Vorrichtung nach Anspruch 1, die ferner eine Einrichtung (120) zum Erzeugen eines Sicherheitsparameters T aufweist,

wobei die Einrichtung (110) zum Erzeugen der fünften Hilfsgröße Mp ausgebildet ist, um die fünfte Hilfsgröße folgendermaßen zu berechnen:

$$Mp = c^{dp'} \bmod (pT); \text{ und}$$

wobei die Einrichtung (112) zum Erzeugen der sechsten Hilfsgröße Mq ausgebildet ist, um die sechste Hilfsgröße Mq folgendermaßen zu berechnen:

$$Mq = c^{dq'} \bmod (q \times T).$$

3. Vorrichtung nach Anspruch 2, die ferner eine Einrichtung zum Berechnen einer siebten Hilfsgröße H7 aufweist, wobei die siebte Hilfsgröße H7 folgendermaßen definiert ist:

$H7 = Mp \times Mq \bmod T$; und

bei der ferner eine Einrichtung zum Berechnen einer achten Hilfsgröße H8 vorgesehen ist, wobei die achte Hilfsgröße H8 folgendermaßen definiert ist:

$$H8 = c^{(dp'+dq')\bmod(T-1)} \bmod T; \text{ und}$$

eine Einrichtung zum Vergleichen der siebten und der achten Hilfsgröße, wobei die Einrichtung zum Vergleichen angeordnet ist, um auf einen Fehler hinzuweisen, wenn die siebte und die achte Hilfsgröße unterschiedlich sind.

4. Vorrichtung nach einem der vorhergehenden Ansprüche, die für eine RSA-Entschlüsselung oder RSA-Signatur vorgesehen ist, wobei m eine Klartextnachricht ist, wobei d ein geheimer Schlüssel ist, und wobei c eine verschlüsselte Nachricht ist.

5. Vorrichtung zum Berechnen eines Ergebnisses einer modularen Exponentiation, wobei n ein Modul ist, wobei d ein Exponent ist, und wobei c eine Größe ist, die der modularen Exponentiation zu unterziehen ist, mit folgenden Merkmalen:

einer Einrichtung (100) zum Berechnen einer ersten Hilfsgröße dp, wobei dp folgendermaßen definiert ist:

$$dp = d \bmod (p - 1),$$

wobei p eine erste Primzahl ist;

einer Einrichtung (102) zum Berechnen einer zweiten Hilfsgröße dq, wobei dq folgendermaßen definiert ist:

$$dq = d \bmod (q - 1),$$

wobei q eine zweite Primzahl ist,

wobei ein Produkt aus p und q gleich dem Modul n ist;

eine Einrichtung (104) zum Bereitstellen eines Sicherheitsparameters T;

einer Einrichtung zum Erzeugen einer dritten Hilfsgröße p x T und einer vierten Hilfsgröße q x T;

einer Einrichtung (110) zum Erzeugen einer fünften Hilfsgröße Mp, wobei die fünfte Hilfsgröße Mp folgendermaßen definiert ist:

$$Mp = c^{dq} \bmod (p \times T);$$

einer Einrichtung (112) zum Erzeugen einer sechsten Hilfsgröße Mq, wobei die sechste Hilfsgröße Mq folgendermaßen definiert ist:

$$Mq = c^{dq} \bmod (q \times T); \text{ und}$$

einer Einrichtung (114) zum Berechnen des Ergebnisses der modularen Exponentiation m, wobei m folgendermaßen definiert ist:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

6. Vorrichtung nach Anspruch 5, bei der der Sicherheitsparameter T eine Primzahl ist.

7. Vorrichtung nach Anspruch 3 oder 5, bei der der Sicherheitsparameter T klein im Vergleich zu der ersten Primzahl p bzw. zu der zweiten Primzahl q ist.

8. Verfahren zum Berechnen eines Ergebnisses einer modularen Exponentiation, wobei n ein Modul ist, wobei d ein Exponent ist, und wobei c eine Größe ist, die der modularen Exponentiation zu unterziehen ist, mit folgenden Schritten:

Berechnen (100) einer ersten Hilfsgröße dp, wobei dp folgendermaßen definiert ist:

$$dp = d \bmod (p - 1),$$

wobei p eine erste Primzahl ist;

Berechnen (102) einer zweiten Hilfsgröße dq, wobei dq folgendermaßen definiert ist:

$$dq = d \bmod (q - 1),$$

wobei q eine zweite Primzahl ist,

wobei ein Produkt aus p und q gleich dem Modul n ist;

Bereitstellen (104) einer Zufallszahl (IRND);

Erzeugen (106) einer dritten Hilfsgröße dp´, wobei dp´ folgendermaßen definiert ist:

$$dp' = IRND \times (p - 1) + dp;$$

Erzeugen (108) einer vierten Hilfsgröße dq´, wobei dq´ folgendermaßen definiert ist:

$$dq' = IRND \times (q - 1) + dq;$$

Erzeugen (110) einer fünften Hilfsgröße Mp, wobei die fünfte Hilfsgröße Mp folgendermaßen definiert ist:

$$Mp = c^{dp'} \bmod p;$$

Erzeugen (112) einer sechsten Hilfsgröße Mq, wobei die sechste Hilfsgröße Mq folgendermaßen definiert ist:

$Mq = c^{dq'} \bmod q$; und

Berechnen (114) des Ergebnisses der modularen Exponentiation m, wobei m folgendermaßen definiert ist:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

10. Verfahren zum Berechnen eines Ergebnisses einer modularen Exponentiation, wobei n ein Modul ist, wobei d ein Exponent ist, und wobei c eine Größe ist, die der modularen Exponentiation zu unterziehen ist, mit folgenden Schritten:

Berechnen (100) einer ersten Hilfsgröße dp, wobei dp folgendermaßen definiert ist:

$$dp = d \bmod (p - 1),$$

wobei p eine erste Primzahl ist;

Berechnen (102) einer zweiten Hilfsgröße dq, wobei dq folgendermaßen definiert ist:

$$dq = d \bmod (q - 1),$$

wobei q eine zweite Primzahl ist,

wobei ein Produkt aus p und q gleich dem Modul n ist;

Erzeugen (104) eines Sicherheitsparameters T;

Erzeugen einer dritten Hilfsgröße p x T und einer vierten Hilfsgröße q x T;

Erzeugen (110) einer fünften Hilfsgröße Mp, wobei die fünfte Hilfsgröße Mp folgendermaßen definiert ist:

$$Mp = c^{dp} \bmod (p \times T);$$

Erzeugen (112) einer sechsten Hilfsgröße Mq, wobei die sechste Hilfsgröße Mq folgendermaßen definiert ist:

$$Mq = c^{dq} \bmod (q \times T); \text{ und}$$

Berechnen (114) des Ergebnisses der modularen Exponentiation m, wobei m folgendermaßen definiert ist:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

Zusammenfassung

Vorrichtung und Verfahren zum Berechnen eines Ergebnisses einer modularen Exponentiation

Bei einer Vorrichtung zum Berechnen eines Ergebnisses einer modularen Exponentiation wird der chinesische Restsatz (CRT) verwendet, bei dem unter Verwendung von zwei Hilfsexponenten und zwei Untermodulen zwei Hilfs-Exponentiationen berechnet werden. Um die Sicherheit der RSA-CRT-Berechnung gegenüber kryptographischen Attacken zu verbessern, wird eine Randomisierung der Hilfs-Exponenten und/oder eine Veränderung der Untermodule durchgeführt. Damit ist eine sichere RSA-Entschlüsselung bzw. RSA-Verschlüsselung mittels des rechenzeiteffizienten chinesischen Restsatzes gegeben.

Figur 1

Figur zur Zusammenfassung

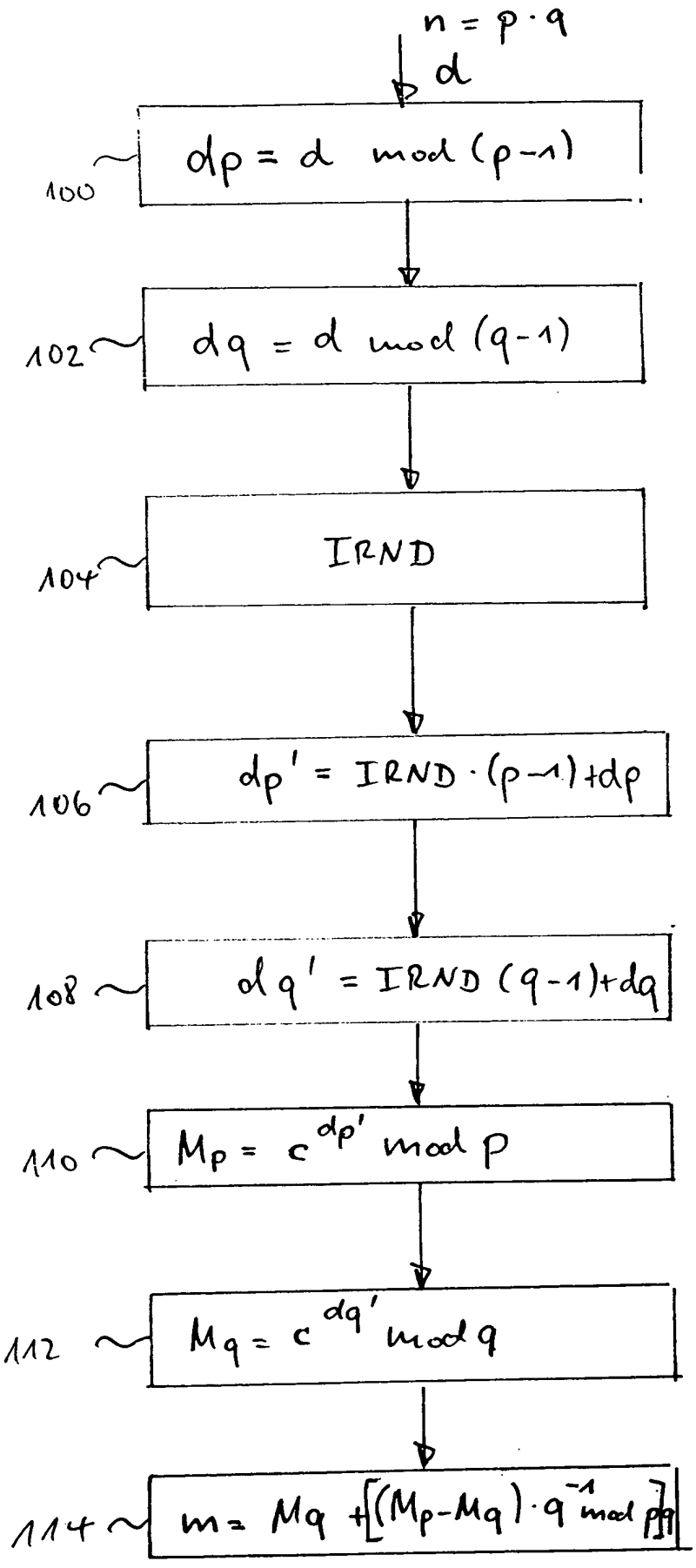


Fig. 1

Bezugszeichenliste

100 Einrichtung zum Berechnen einer ersten Hilfsgröße dp
102 Einrichtung zum Berechnen einer zweiten Hilfsgröße dq
104 Einrichtung zum Erzeugen einer Zufallszahl IRND
106 Einrichtung zum Erzeugen einer dritten Hilfsgröße dp´
108 Einrichtung zum Erzeugen einer vierten Hilfsgröße dq´
110 Einrichtung zum Berechnen einer fünften Hilfsgröße Mp
110´Einrichtung zum Erzeugen der fünften Hilfsgröße Mp unter Verwendung eines veränderten Untermoduls
112 Einrichtung zum Berechnen einer sechsten Hilfsgröße Mq
112´Einrichtung zum Erzeugen der sechsten Hilfsgröße Mq unter Verwendung eines veränderten Untermoduls
114 Einrichtung zum Berechnen des Ergebnisses der modularen Exponentiation
120 Einrichtung zum Erzeugen des Sicherheitsparameters T
140 Einrichtung zum Berechnen einer siebten Hilfsgröße H7 und einer achten Hilfsgröße H8
142 Einrichtung zum Bestätigen der Übereinstimmung der siebten und achten Hilfsgröße
144 Einrichtung zum Hinweisen auf einen Fehler im CRT
200 Erhalten des öffentlichen Schlüssels
210 Darstellen der Nachricht als Zahl
220 Berechnen von c
230 Ausgeben von c
240 Kanal
250 Empfangen von c
260 Berechnen von m

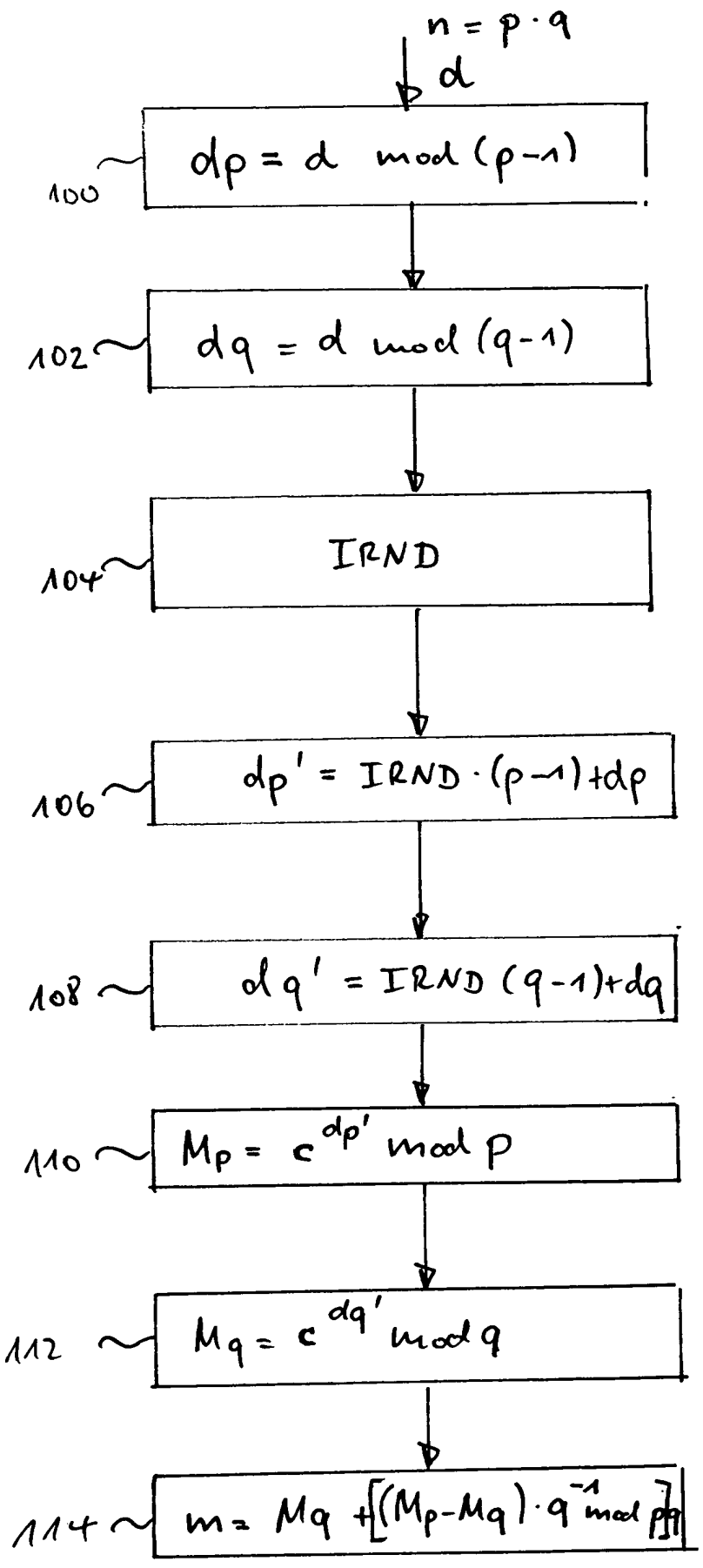

n = p · q
d
100
dp = d mod (p-1)
102
dq = d mod (q-1)
104
IRND
106
dp' = IRND · (p-1) + dp
108
dq' = IRND (q-1) + dq
110
Mp = c^dp' mod p
112
Mq = c^dq' mod q
114
m = Mq + [(Mp - Mq) · q^-1 mod p] q

Fig. 1

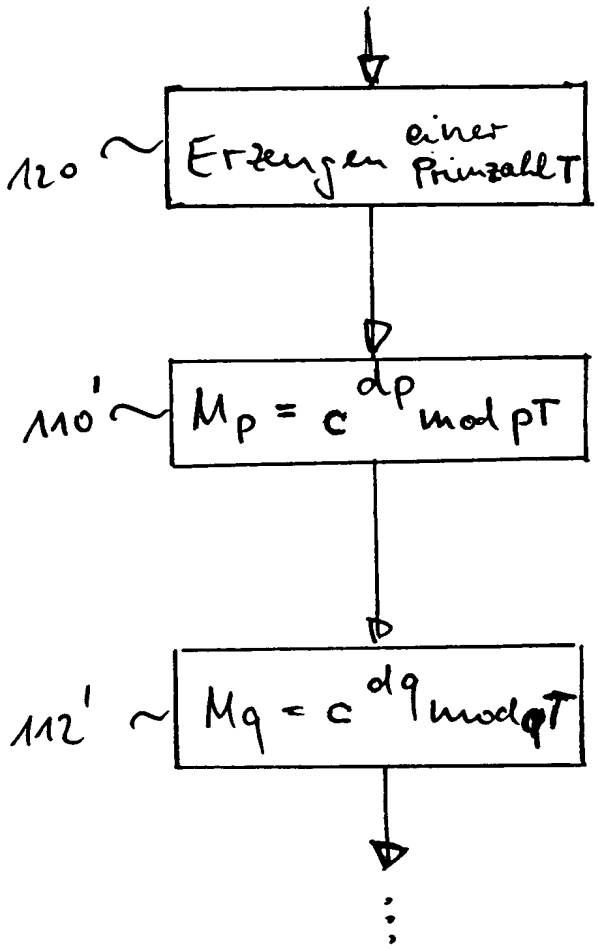

120
Erzeugen einer Primzahl T
110'
$M_p = c^{d_p} \bmod pT$
112'
$M_q = c^{d_q} \bmod qT$

Fig. 2a

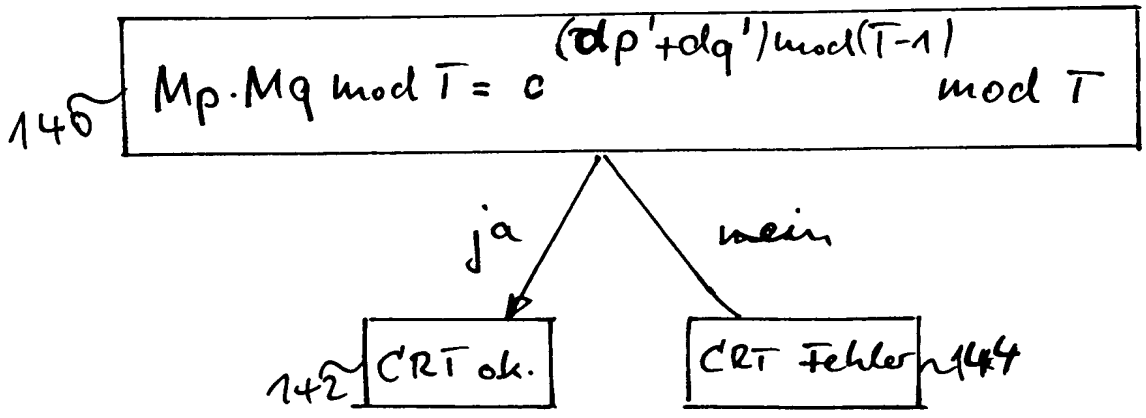

140
$M_p \cdot M_q \bmod T = c^{(d_p' + d_q')/\bmod(T-1)} \bmod T$
ja
nein
142
CRT ok.
CRT Fehler
144

Fig. 2b

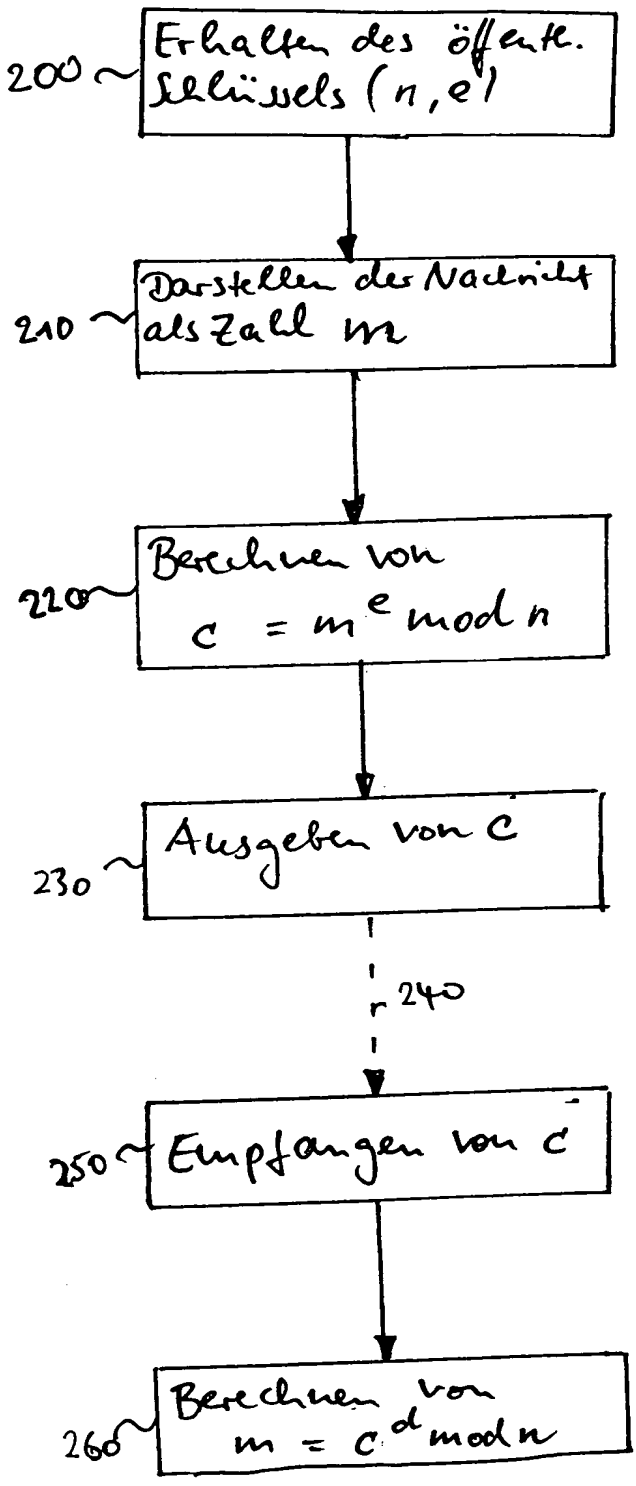


Fig. 3 (Stand der Technik)